文章编号: 2095-0365(2010)04-0018-04

科技奖励评审系统中专家身份认证功能的设计与实现

胡畅霞, 刘晓星, 韩立华, 石玉晶

(石家庄铁道大学 信息科学与技术学院, 河北　石家庄　050043)

摘　要: 对科技奖励评审系统中实现身份认证时带来的安全问题进行了分析, 提出并在该系统中实现了一种改进的身份认证方案——二次校验技术。实践证明, 该技术的使用极大提高了系统的安全性。

关键词: 安全; 加密; 身份认证

中图分类号: TP311.52　　文献标识码: A

一、引言

河北省科学技术奖励网络评审系统的研究目标是面向全省科技奖励工作构建能满足河北省评审需要的、本土化的、人性化、可定制、安全性高的科技奖励平台, 实现对河北省突出贡献奖、自然科学奖、技术发明奖、科技进步奖和国际合作奖等五个奖种的全程无纸化的计算机综合业务处理及全面的网络评审。通过该系统的使用, 能极大简化工作业务, 提高工作效率, 降低政府运作成本, 实现公平、公正、公开的科技奖励监督机制, 提高办公效率和服务管理质量。

专家身份认证是科技奖励评审系统中最基本的安全保护手段, 其目的是确定某一专家的身份, 以确定专家的访问权限。为了能充分发挥科技奖励评审系统的各项功能, 必须具有一个安全、方便的身份认证系统。

二、身份认证的现状分析

一般来说, 用户身份认证可通过三种基本方法或其组合方式来实现[1]:

(1) 用户所知的某个秘密信息, 例如用户知道自己的口令。

(2) 用户持有的某个秘密介质, 用户必须持有合法的随身携带的物理介质, 例如智能卡中存储用户的个人化参数, 访问系统资源时必须要有智能卡。

(3) 用户所具有的某些生物学特征, 如指纹、声音、DNA 图案、视网膜扫描等等, 但这种方案一般造价较高, 适用于保密程度很高的应用领域。

本项目在设计之初采用的是方式(1): 专家在填写专家号和登录口令后(注: 专家初次登录时, 登录口令是由系统自动生成的, 专家登录成功后可修改密码), 首先将信息送至 Web 服务器, Web 服务器将得到的信息作为被验证内容添加至执行模块, 模块中有负责和数据库服务交互的代码, 该代码负责将专家所填写的专家号在数据库中对应的口令取出并和该专家所填写口令进行对比, 此过程全部由 Web 服务器操纵, 口令相同的则允许登录。为了防止黑客使用特定程序暴力破解方式进行不断的登录尝试, 在专家登录的时候还需进行验证码校验。所谓的验证码校验[2], 就是当用户访问 Web 服务器请求进入登录界面的时候, 服务器在响应客户端请求的同时, 生成一串随机产生的数字或者符号, 并且将这一串数字或符号生成一幅图片, 图片里加上一些干扰像素以防止 OCR, 将这幅图片与响应内容一同发到客户端浏

收稿日期: 2010-09-03

作者简介: 胡畅霞(1977–), 女, 讲师, 研究方向: 网络与信息安全。

览器上, 由用户肉眼识别其中的验证码信息, 填入验证码框, 然后提交给服务器验证, 验证成功后才能使用相应功能。

这种认证方式需要专家号、登录口令及校验码同时验证, 对专家身份起到了一定的作用, 但采用此方法的弊端在于口令保存的安全性问题和口令的防攻击性问题。为了进一步提高系统的安全性, 需在原认证方式的基础上进行改进。

三、专家身份认证功能的设计与实现

(一) 功能设计思路

本系统在原认证方式的基础上进行了改进, 采用了"二次校验"技术: 系统仍将通过专家号、登录口令和校验值对专家身份进行验证, 并赋予其不同的权限以对系统进行不同的操作。与原认证方式不同, 这里的校验值是由系统根据专家身份信息利用加密算法唯一生成的。

加密算法 MD5 与 SHA-1 均是从 MD4 发展而来, 它们的结构和强度等特性有很多相似之处。SHA-1 对抗强行攻击的强度更大, 但由于 SHA-1 的循环步骤比 MD5 多(80: 64) 且要处理的缓存大(160 比特: 128 比特), 因此 SHA-1 的运行速度比 MD5 慢[3]。鉴于此, 本系统采用的是 MD5 加密算法。当专家登录时, 输入专家号、口令和校验值后, 除了原有的专家号和口令认证外, 还要进行校验值的比对。

(二) 功能实现

在网络评审之前, 由管理员操作后台程序主要进行两步操作:

1. 为专家批量生成校验码

(1) 系统首先读取数据库中的专家编号(F_ZJBH), 为了进一步加强保密性, 在专家编号 F_ZJBH 后又加上了一个随机数 Rsu 并以此作为生成校验值的字符串, 然后利用 MD5 算法进行加密, 即 Hi= MD5(Rsu, F_ZJBH), 生成 32 个字符的信息摘要, 最后随机截取其中的 8 位存入 T_DLJY_TEMP(登录校验临时表), 作为第 2 步发给专家的登录校验码。

(2) 为了确保安全性, 对第一步生成的 8 位校验码再次进行 MD5 散列, 并存入 T_DLJY(登录校验表); 当专家通过网站登录并输入第一步的 8 位校验码后, 将会对此校验值进行 MD5 散列, 系统将得到的散列值和数据库 T_DLJY 中的字段 F_MD5 进行比较, 只有两者匹配才允许登录。

2. 编辑短信并群发短信

(1) 设置并连接短信猫: 选择短信猫的 USB 端口(默认), 发送速度、发送条数(条/小时)。

(2) 点击【编辑短信】按钮, 定制短信内容, 形成包含专家名和校验值的短信。

(3) 选择专家, 将编辑好的短信内容群发给专家, 此步关键要调用短信猫提供的 API 接口函数 Sms_Send[4], 格式如下:

Sms_Send(Sms_TelNum As String, Sms_Text As String) As Integer

功能描述: 发送短信。其中 Sms_TelNum: 发送给的终端号码; Sms_Text: 发送的短信内容; Sms_Send: 返回值(0: 发送短信失败; 1: 发送短信成功)。

利用后台程序生成校验码及群发短信的流程图如图 1 所示。专家登录网站时的验证流程以网评阶段为例:

(1) 第一次校验。①专家输入自己所属的网评组号, 专家编号、登录口令及手机上收到的 8 位校验码。②服务器根据专家输入的网评组号、专家号和登录口令查询是否有此专家信息, 若没有, 校验结束, 此身份认证失败; 若有, 则到(2)。

(2) 第二次校验。将 8 位校验码进行 MD5 散列, 得到的值与数据库中存储的散列值进行比较, 若匹配, 则身份验证成功; 若否, 则失败。

四、关键问题

专家身份认证模块是实现整个系统安全性能的重要保证, 在这个模块加入了二次校验来替代原来系统随机生成的校验值, 在设计时主要考虑两个关键问题:

(一) 获取专家的哪些信息来进行 MD5 散列

对专家的信息进行 MD5 校验, 需获取每位专家唯一的信息——专家号, 但 MD5 散列时只使用专家号, 考虑到非法人员若得知这一信息时会以同样的方式获取 MD5 校验值, 则无保密性可言。因此系统实现时, 在每个专家号的后面又加上了一个随机数字符串, 这样非法人员就无法通过专家信息来获取 MD5 校验值, 从而进一步增强了系统的保密性和安全性。

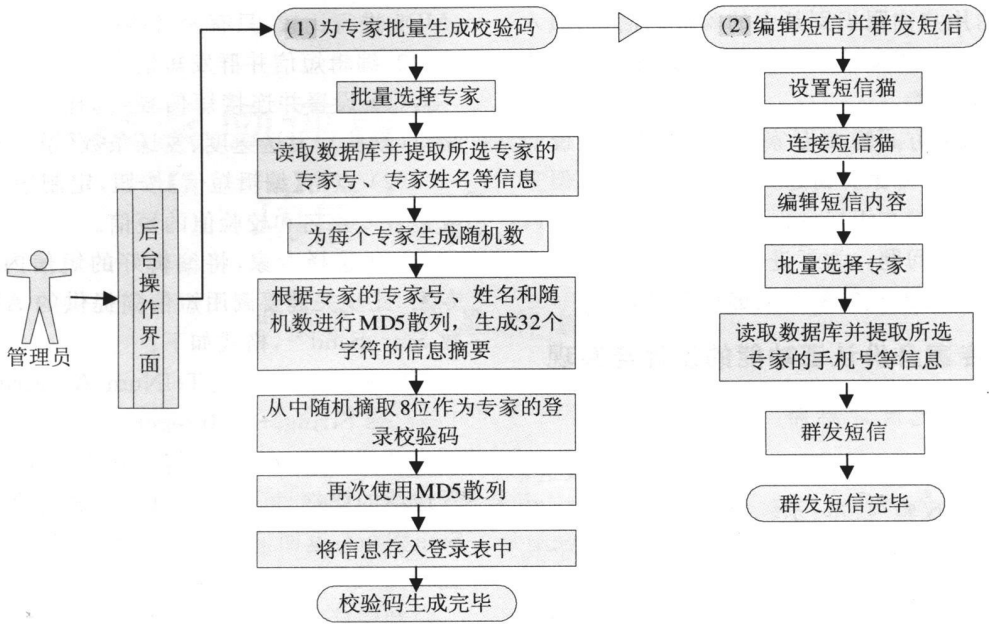

图1 后台生成校验码及群发短信流程图

(二)如何防止有人非法进入数据库窃取专家校验值

如果生成的校验值直接存放在数据库登录表中,当专家登录时进行校验,其实是和密码认证方式没有太大区别,唯一的不同是这里的校验值是系统生成的,而密码是由专家本人设定的。因此数据库表中不能直接存储专家登录的校验码。

为解决该问题则需要存储一个中间值,这个值是专家登录所要输入校验值的再次MD5校验值。非法人员若非法读取数据库时能看到这个中间值,但不能得到专家登录时的校验值,保密性进一步增强。然而,随之而来的问题是如何将校验值通知专家,因为数据库中存储的校验值并不能登录系统。系统实现时的解决方法是在数据库中建立一张临时表,用来存储专家登录时需要输入的校验值,并用短信告知专家。

系统中的网评、行评等功能模块的专家登录都是有时间限制的,因此在一定的时间段,可以是短信告知全部专家且确认专家已收到后,然后删除临时表,以此来解决了保密问题。

采用二次校验技术的优点如下:

(1)在身份认证数据中,对每个用户引入了随机数和专家号相结合完成的消息摘要生成过程,这样增加了攻击者攻击口令的难度。并且不同的用户对应不同的随机数,这样即使攻击者得到了随机数和消息摘要,它可以将各种长度的字符组合和用户所使用的随机数合并起来计算消息摘要,但是这个随机数只在这一个口令中有效,其它口令使用的是其他随机数,攻击者的计算量是非常巨大的。

(2)采用了二次校验,即数据库中校验值字段存储的不是专家登录时所输入的校验值,而是此校验值再次散列的校验值,即便有人非法进入数据库也不能获得专家的校验值,进一步提高了系统的安全性。

五、结语

目前该系统已成功应用于河北省、沧州市等科技奖励评审部门,即将在省内各地市全范围推广。通过实践证明,采用本身份认证方式后,大大提高了系统的稳定性和可靠性。

参考文献:

[1]宁洁琪. 基于MD5二重加密的安全技术探讨[J]. 广西轻工业,2009,25(10):78-79.

[2]段钢. 加密与解密[M]. 北京:电子工业出版社,2008:50-52.

(下转第95页)

参考文献:

[1] 吴镝. 从博雅教育、通识教育到人文素质教育[J]. 南京理工大学学报: 社会科学版, 2004, 17(2): 71-76.
[2] 邬川雄. 文化移植、传承与创新? ——从西方大学的博雅教育传统看台湾通识教育[J]. 通识教育与跨域研究, 1997(5): 23-56.
[3] 江学建, 蔡加成. 大学课程设置体现的中西文化差异——国内外大学创新教育比较研究[J]. 教育与现代化, 2006(1): 26-32.
[4] 代曦. 我国理工科高等院校文化素质课程设置现状分析[EB/OL]. http://www.pep.com.cn. 2008-4-29.
[5] 羊城晚报. 中山大学五千新生率先体验"通识教育"[EB/OL]. 中国新闻网, 2009-8-26.
[6] 张喜梅, 张雪菲. 麻省理工学院的通识教育对理工大学课程设置的启示[J]. 中国冶金教育, 2005(2): 42-46.
[7] 张燕. 浅析"博雅教育"[J]. 四川师范大学学报: 社会科学版, 2005, 5(增刊): 209-210.
[8] 魏善春. 博雅教育视野下对大学教育改革的思考[J]. 教育探索, 2009(9): 69-70.
[9] 阎立钦. 创新教育——面向 21 世纪我国教育与发展的抉择[M]. 北京: 教育科学出版社, 1999.

Comparative Analysis of Characteristics of College Liberal Education in China and Abroad

——Also on college liberal education Form and system construction in China

ZHU Tao-xing[1,3], ZHU Zheng-guo[3], ZHAO Li-qin[2], WU Dian-ting[2]

(1. Schoole of Economics and Management, Sshijiazhuang Tiedao University, Shijiazhuang 050043, China;
2. School of Civil Engineering, Sshijiazhuang Tiedao University, Shijiazhuang 050043, China;
3. College of Geography and Remote Sensing Science, Beijing Normal University, Beijing 100875, China)

Abstract: This paper analyzes liberal arts of the ancient and modern tradition, puts forward the definitions of liberal education, general education and quality education in substance. This paper also comparative analyzes the form of education and curriculum, and concludes the necessity of liberal education, and suggesting building a liberal arts education system with Chinese traditional characteristics.

Key words: liberal education; general education; colleges and universities; curriculum provision

(上接第 20 页)

[3] 武新华, 安向东, 苏雅, 等. 加密解密全方位学习[M]. 北京: 中国铁道出版社, 2006: 30-35.
[4] 欧阳元东. 基于 ASP.NET 的 WEB 平台发送手机短信的技术实现[J]. 福建电脑, 2009(3): 150-151.

Design and Implementation of Experts Identity Authentication in Science and Technology Award Assessment System

HU Chang-xia, LIU Xiao-xing, HAN Li-hua, SHI Yu-jing

(School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang 050043, China)

Abstract: The problem of identity authentication in the science and technology award assessment system is analyzed in the paper. A kind of improved identification scheme, the second calibration technique, is put forward and realized. Practice proves that the use of this new technology has greatly increased the security of the system.

Key words: security; encryption; identity authentication